electronics

MDPI

*Article*

# Security and Trust in the 6G Era: Risks and Mitigations

**Giulio Tripi , Antonio Iacobelli , Lorenzo Rinieri and Marco Prandini ***

Department of Computer Science and Engineering (DISI), Alma Mater Studiorum—Università di Bologna, 40136 Bologna, Italy; giulio.tripi@unibo.it (G.T.); antonio.iacobelli@unibo.it (A.I.); lorenzo.rinieri@unibo.it (L.R.)
* Correspondence: marco.prandini@unibo.it

**Abstract:** The ubiquitous diffusion of connected devices in every context of the daily life of citizens, public bodies, and companies is stimulating the creation of new applications that require very high wireless communication performances. To fulfill this need, the sixth generation of communication standards (6G) is planned to roll out by 2030. While structuring this new standard, it is crucial to take into account the security aspects given the impact of the technologies that will rely on its reliability and resiliency. In this paper, we provide an overview of the technologies that will be used in 6G to achieve the required functional goals for the development of key applications. Then, we proceed to discuss the threats and the solutions to make the communications infrastructure secure and reliable, and finally, we elaborate on the concept of how to achieve trust in this scenario.

**Keywords:** 6G; security; trust; wireless networks; blockchains

**Citation:** Tripi, G.; Iacobelli, A.; Rinieri, L.; Prandini, M. Security and Trust in the 6G Era: Risks and Mitigations. *Electronics* **2024**, *13*, 2162. https://doi.org/10.3390/electronics13112162

Academic Editors: Changhoon Lee, YoHan Park, Tao Huang, Tsz Hon Yuen, Guanglin Zhang, Shihao Yan and Jusak Jusak

Received: 30 April 2024
Revised: 24 May 2024
Accepted: 31 May 2024
Published: 1 June 2024

## 1. Introduction

The advent of 6G technology heralds a new era in mobile networking, promising unparalleled speed, connectivity, and potential for innovation. As the successor to 5G, 6G is not merely an incremental upgrade but a quantum leap forward, aiming to address the escalating demands of network traffic driven by the proliferation of mobile devices, Internet of Things (IoT) applications, smart city initiatives, and the burgeoning requirements of emerging technologies.

Notwithstanding the slow adoption of 5G, which has not yet fully replaced 4G [1], the first studies concerning a sixth-generation wireless network are beginning to take shape. First conceptualized as soon as 5G was standardized, the vision for 6G was born out of the recognition that existing infrastructure would soon face limitations in managing the exponential growth in data traffic and the need for ultra-low latency and broader network coverage demanded by future technologies. To satisfy these new requirements, new technologies should be developed in order to address issues spread over the full stack, ranging from the physical problems of the wireless frequencies to the adoption of highly automated management paradigms.

The potential applications of 6G are as vast as they are revolutionary, promising to reshape industries and redefine human interaction with technology. From multisensory eXtended Reality (XR) experiences to the seamless coordination of Connected Robotics and Autonomous Systems (CRAS), and from Wireless Brain–Computer Interactions (BCI) to the secure deployment of Blockchain and Distributed Ledger Technologies (DLT), there are lots of implementations that could benefit from 6G technology.

At the heart of 6G lies a trifecta of transformative technologies: Reconfigurable Intelligent Surfaces (RIS), Visible Light Communication (VLC), and the integration with Artificial Intelligence (AI). RIS offers a solution to the limitations of high-frequency transmissions, enhancing signal propagation and stability by utilizing surfaces that intelligently reflect and redirect signals. Meanwhile, VLC leverages visible light to achieve high-speed data transmission, promising seamless integration with existing infrastructure and negligible impact on human health.

The fusion of 6G with Artificial Intelligence marks a paradigm shift in network management, enabling the real-time optimization of resources, dynamic spectrum management, and robust cybersecurity measures. The role of AI extends beyond mere optimization, empowering networks to predict and adapt to traffic patterns, to seamlessly integrate application demands with network management, and to preempt cyber threats against communications.

In detail, recognizing the imperatives of security, trust, and privacy, the 6G architecture envisages a novel security paradigm, reimagining traditional approaches to safeguard against evolving threats. Divided into distinct layers—the physical layer, connection layer, and application layer—6G's security architecture adopts a multi-pronged approach to address vulnerabilities and mitigate risks.

In the physical layer, where the hardware foundation of 6G systems resides, innovative solutions such as Reconfigurable Intelligent Surfaces and Friendly Jamming offer robust defenses against eavesdropping, jamming, and spoofing attacks. These technologies not only enhance signal integrity but also render interception virtually impossible, ensuring the confidentiality of communications.

Meanwhile, at the connection layer, technologies such as Quantum Key Distribution (QKD), Network Slicing, and Intrusion Detection Systems (IDS) bolster defenses against a spectrum of threats, from Denial of Service (DoS) attacks to Man-in-the-Middle (MitM) and Replay attacks. These technologies not only fortify network integrity but also lay the groundwork for dynamic, adaptive security measures capable of thwarting emerging threats in real time.

At the top of the stack, in the application layer, Quantum Homomorphic Cryptography (QHC) and Authentication and Key Agreement (AKA) could be used to protect from threats like social engineering that take advantage of the victim's naivety.

As the 6G landscape continues to evolve, our approach to security, trust, and privacy must evolve alongside it. Concepts such as Zero Trust Architecture (ZTA), Distributed Ledger Technologies (DLT), and Trust Anchors offer a glimpse into the future of network security, promising a paradigm shift from perimeter-based defenses to a dynamic, risk-based approach that scrutinizes every interaction, device, and user within the network.

In the journey toward 6G, security is not merely a feature—it is a fundamental prerequisite for realizing the transformative potential of next-generation telecommunications. As we embark on this journey, the fusion of innovation and security will pave the way for a future where connectivity is not just fast and ubiquitous but also resilient, trustworthy, and secure.

The structure of this paper is outlined as follows: the next section gives the motivation for our work with respect for related ones, then in Section 3 we delve into the challenges, technologies, and application scenarios pertinent to 6G. Subsequently, Sections 4–6 scrutinize security and trust considerations across the physical, connection, and application layers, respectively. Lastly, in Section 7, we offer a comprehensive conclusion, summarizing the key findings and contributions of this study.

## 2. Motivations and Related Works

This section presents a summary of existing surveys on the subject and highlights our motivation for this work. The first contribution regards breadth: various surveys have dealt with key issues about 6G, including security, trust, and privacy. However, these surveys often focus on specific 6G areas, such as quantum security technologies [2], AI-driven security [3,4] and trusted networks [5]. These are considered to be the main 6G priorities. The second contribution instead tackles depth: other studies have conducted analyses of only one specific layer. For instance, in [6–8], the security measures concerning the physical layer are treated in detail. In [9], the potential security and privacy challenges in various 6G technologies and applications are highlighted but without focusing on the trust aspect. Finally, Nguyen et al. [10] propose a review of the security and privacy of 6G, which is divided into levels. However, the paper does not delve deeply into the trust aspects. Consequently, there is no comprehensive survey that provides a holistic view of

6G security, privacy, and trust issues in the context of the overall security architecture. Our work therefore aims to fill this gap, as we believe that treating security, privacy, and trust issues in different layers allows network and security practitioners and researchers to apply the concept of defense in depth to security design. This approach permits the design of network security in an end-to-end manner as opposed to a piecemeal approach to securing the network against attacks. Furthermore, the layered approach to security can assist in addressing conflicting objectives, such as the prioritization of security through encryption and network intelligence.

## 3. The Dawn of 6G

The term 6G refers to the sixth generation of mobile networking, not yet implemented, which was first discussed in [11], right before the roll-out of 5G. The idea behind 6G is the need to manage a rapid growth of network traffic due to the proliferation of mobile devices (not only mobile phones but also IoT, smart city, smart manufacturing, and smart mobility) and the request for a fast and stable connection. In addition, new technologies are rising which require a latency unreachable with today's 5G implementation [12]. In the following sections, we will describe the technologies that 6G will use to overcome the limitations of 5G, the application scenarios that require the performance enhancements that 6G will provide, and the security and privacy concerns in 6G, without forgetting an analysis on trust between the actors on the network.

### *3.1. Technologies*

The 6G technology aims to improve wireless connectivity overcoming actual and future challenges relying on new technologies that are only theorized at the moment. The new technologies that will be used to provide the performance required by 6G are clearly described in [13]; for the sake of readability, we summarize them here:

- Reconfigurable Intelligent Surfaces (RIS): very high frequencies, beyond 100 GHz and up to a few THz [14], will be used by 6G to achieve high-speed data transmission. However, this comes with some limitations from the coverage point of view. In fact, high frequencies have a lower range and they cannot penetrate obstructions as well as lower frequencies can. Thus, to address these limitations, reflective surfaces known as RIS could be employed. These surfaces reflect signals from the sender circumventing obstacles, redirecting them to the receiver intact. As depicted in Figure 1, RIS could be Reflective, meaning that they reflect the signal in a specific direction to improve the route of the signal, or Transmissive, that is they transmit the signal by modulating and controlling it with its constituent elements. Furthermore, thanks to their versatility and scalability, they would fit seamlessly into existing networks without changing any protocols or hardware components and would cost very little for their functionality. RIS can also be useful in trying to counteract the Doppler effect [15], thus allowing a stable connection even to fast-moving devices.
- Visible Light Communication (VLC): VLC is a high-speed wireless communication technology based on the employment of visible light to transmit data. In particular, it uses LED lights to modulate visible light using a very high bandwidth with a frequency of 400–800 THz, which is much higher than the radio frequencies. VLC is a good alternative to standard wireless communication because it allows transfering large amounts of data with existing lighting systems with negligible costs and no harm to human health [16].
- Artificial Intelligence applied to 6G: The exponential development of AI in recent years will inevitably affect 6G technologies, bringing significant advantages to communication networks. In particular, Artificial Intelligence can be used to improve and automate various aspects of IT operations (AIOps-enabled) [17]. These solutions are designed to cope with the complexity and scale of modern IT environments, facilitating the management of infrastructure, applications, and services and allowing the detection of any anomalies. Furthermore, the application of Artificial Intelligence can

be employed for real-time resource management and optimization within networks (Self-Optimizing Networks). This includes enhancing traffic flow, connection speed, and forecasting traffic peaks to proactively manage them. Additionally, it will enable dynamic frequency allocation planning (Dynamic Spectrum Management) [13] and mitigate interference issues. Finally, the application of AI on a large scale will result in a notable increase in the costs associated with training and the collection of large-scale datasets. Consequently, it becomes imperative to utilize specialized AI approaches such as federated learning [18], which facilitate the coordination of the learning process across millions of distributed devices to enhance the quality of the centralized learning model (global federated learning model).

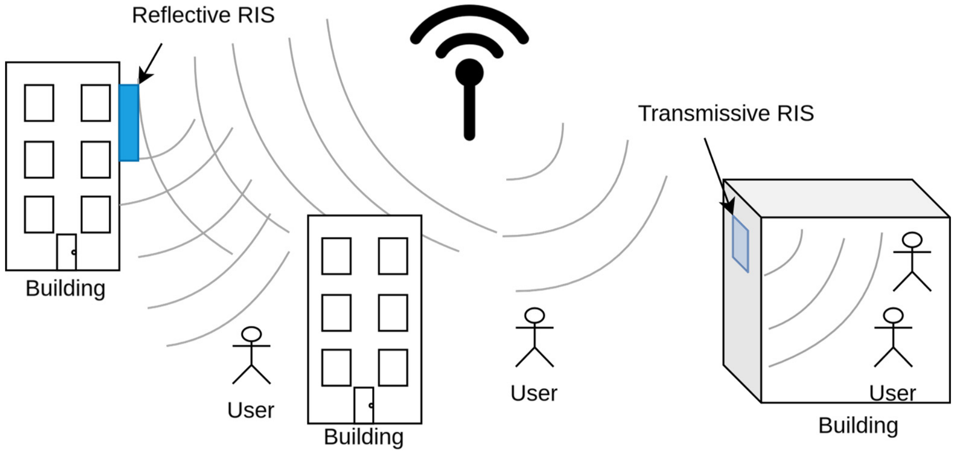

**Figure 1.** Examples of reflecting and transmitting Reconfigurable Intelligent Surfaces.

### *3.2. Application Scenarios*

The 6G features enable a wide range of innovative applications, as illustrated in [19], which can be summarized as follows:

- Multisensory XR: eXtended Reality (XR) is a generic term that is used to the combination of virtual reality (VR), augmented reality (AR) and mixed reality (MR). XR is applicable to rethink how many activities of real life can happen, starting with education, healthcare, and extending to entertainment, combining the physical and digital worlds and allowing users to immerse and interact with objects in a sort of hybrid universe between virtual reality and the real world [20].
- Connected Robotics and Autonomous Systems (CRAS): One of the main objectives of 6G is certainly to enable the maximum efficiency of CRAS. The term refers to a wide range of robotic and autonomous systems connected to each other and to a common network, enabling them to share data, collaborate, and perform tasks independently. CRAS will be crucial for the operation of new services such as autonomous vehicles, remote surgery, environmental and pollution monitoring, industrial automation, and remote rescue operations in disaster-stricken locations.
- Wireless Brain–Computer Interactions (BCI): BCIs are a disruptive technology with respect to how we interact with computers and other devices. Specifically, they are based on certain devices (worn or implanted) that transmit wireless signals corresponding to the user's brain activity, thus allowing them to control local or remote devices without the need for physical contact and taking advantage of 6G connectivity. BCI was previously limited to healthcare contexts, but with 6G, its potential will increase to the point where it will be applicable in many sectors [21].
- Blockchain and Distributed Ledger Technologies (DLT): DLT is a type of decentralized technology that allows data to be recorded and shared among all participants in the network, guaranteeing authenticity and integrity without the need for a central, trusted authority. DLTs can benefit from 6G systems to provide highly scalable and secure networks that are capable of supporting the growing number of devices and

data-intensive applications. In turn, DLTs would provide 6G systems with much more security and transparency in the transfer of data and interactions between devices [22].

### *3.3. Security and Privacy in 6G*

Security, trust, and privacy stand as cornerstones in the foundation of 6G networks. As we embark on the journey toward 6G, it is becoming increasingly evident that the existing security architecture outlined by the 3rd Generation Partnership Project (3GPP) standard [23] will require substantial enhancements to accommodate the myriad innovations poised to redefine the landscape of wireless communication. While the 3GPP standard has been instrumental in shaping the security framework of preceding generations, the advent of 6G necessitates significant changes to address the evolving threat landscape and the unique demands of futuristic applications. In response to this imperative, 6G proposes new technical solutions that build upon the foundational structure laid out by its predecessor, 5G, while incorporating significant adaptations to meet the distinctive requirements of the forthcoming systems. We will analyze those solutions by dividing them into three layers: the physical, connection, and application layers. This hierarchical division aims to provide a comprehensive and layered approach to security, effectively addressing vulnerabilities at each stratum of the network stack.

The physical layer serves as the bedrock upon which the entire network infrastructure is built, encompassing the tangible hardware components and transmission mediums that facilitate the exchange of data. Inherent vulnerabilities at this layer include physical tampering, signal interception, and electromagnetic interference. To mitigate these risks, robust encryption protocols, tamper-evident hardware, and physical security measures are employed to safeguard the integrity and confidentiality of data transmissions.

Moving up the hierarchy, the connection layer serves as the conduit through which data traverses between network nodes, encompassing protocols and procedures governing the establishment and maintenance of communication links. Vulnerabilities at this layer comprise a broad spectrum of threats, including man-in-the-middle attacks, protocol vulnerabilities, and unauthorized access to network resources. Countermeasures such as secure authentication mechanisms, intrusion detection systems, and protocol-hardening techniques are deployed to fortify the resilience of the connection layer against malicious intrusions.

At the apex of the architectural pyramid lies the application layer, the interface through which end-users interact with network services and applications. This layer represents the front-line defense against a diverse array of threats, including malware, social engineering attacks, and data breaches. To safeguard the confidentiality, integrity, and availability of user data, a multifaceted approach to security is employed, encompassing robust authentication mechanisms, data encryption, and behavioral analysis to detect anomalous activities.

In addition to delineating the vulnerabilities inherent in each layer, it is imperative to analyze the types of attacks that may exploit these vulnerabilities and the corresponding countermeasures that can be implemented to mitigate their impact. From sophisticated cyberattacks orchestrated by nation-states to opportunistic exploits perpetrated by cyber criminals, the threat landscape facing 6G networks is multifaceted and constantly evolving. By adopting a proactive stance toward security, leveraging cutting-edge technologies such as Artificial Intelligence, blockchain, and quantum cryptography, and fostering collaboration across industry stakeholders, the vision of a secure, trusted, and privacy-respecting 6G ecosystem can be realized.

### *3.4. Trust in 6G*

Trust in telecommunication systems is a crucial requirement that is intrinsically linked to the security of the information exchanged between devices and users. In particular, trust refers to the relationship between user and machine and could be of two kinds:

- Direct: based on the past interactions between the user and the system;
- Indirect: based on third parties' opinions or recommendations.

Both types of trust play an important role in understanding the level of trustworthiness of a given system; however, it is important to consider that trust is a dynamic concept and can change over time. In 6G, due to the increase in network complexity and the exponential development of the number of interconnections, a significant improvement in trust management is required compared to today's networks, as new 6G systems will lead to the emergence of new threats and vulnerabilities that will have to be effectively countered. For this reason, trust management in 6G will be different from the traditional one, with the implementation of new models and mechanisms, analyzed in the following paragraphs, to guarantee reliability in communications.

The security, trust, and privacy vulnerabilities of each layer are analyzed below with a focus on the types of attacks that can be used and the countermeasures that can be implemented. Figure 2 shows an overview of the aforementioned elements and their division in layers, with each vulnerability linked to its countermeasure.

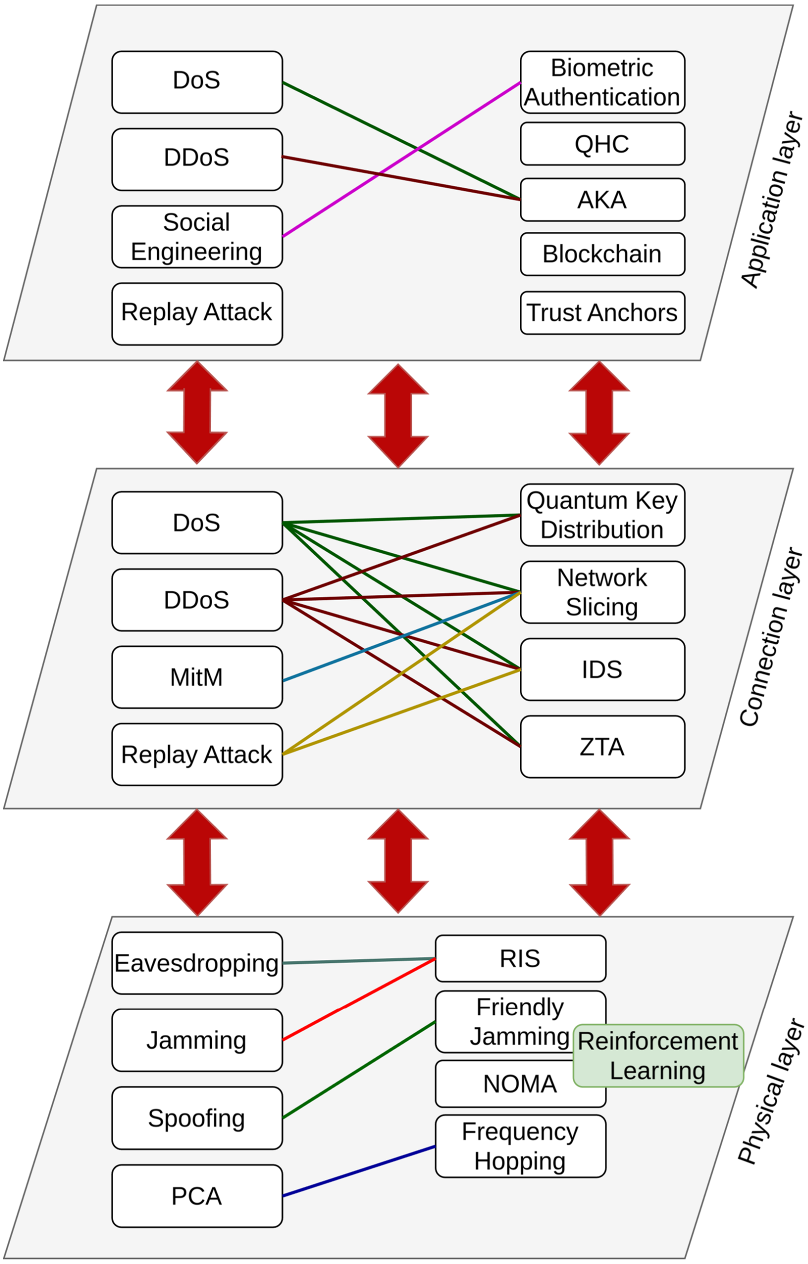

**Figure 2.** Overview of vulnerabilities and solutions layer by layer (link colors added for readability only—no specific meaning).

## 4. Physical Layer

The physical layer is the hardware foundation of 6G systems. Its critical importance is reflected in vulnerabilities that could have fatal consequences for the operation and security of the systems. In particular, the security implemented in this layer must be simple and low cost, so that it can work on devices that do not have high computing power [24]. Figure 3 shows the relations between the mitigations proposed and the security and trust threats.

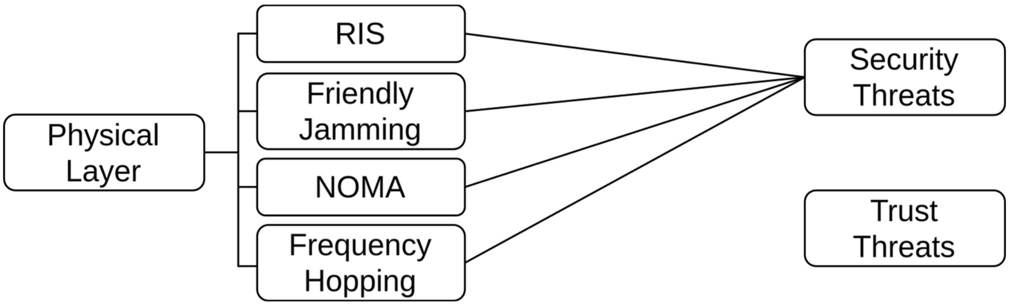

**Figure 3.** Diagram of the mitigations in the physical layer divided by security and trust threats.

### *4.1. Vulnerabilities and Threats*

The most dangerous and widespread attack types in the physical layer of 6G systems will be the following:

- Eavesdropping: this is a type of attack where the attacker eavesdrops on conversations between two parties without authorization and intercepts sensitive information [25].
- Jamming: this attack generates interference signals or noise in the communication channel, making the transmission of information unreliable and disrupting communication [26].
- Pilot Contamination Attack (PCA): this attack “contaminates” the pilot signal from a base station, compromising communications and network performance [27].
- Spoofing: this attack involves spoofing the identity of a person or device to deceive other users or systems and gain unauthorized access [26].

### *4.2. Mitigations*

#### 4.2.1. Reconfigurable Intelligent Surfaces

Reconfigurable Intelligent Surfaces are crucial in avoiding eavesdropping attacks due to their ability to reflect the signal without degrading it. In particular, they can be configured to reflect the signal itself in unpredictable ways, making it almost impossible for the attacker to identify the direction of the signal and intercept it. The effectiveness of this countermeasure increases proportionally to the scale of RIS deployment: the more possible paths for the signal being sent, the more difficult it is for the attacker to identify and intercept the communication. Figure 4 illustrates an example of how RIS, by reflecting the signal in an indeterminate manner, is capable of evading eavesdropping attacks. This is achieved by allowing the communication to traverse two distinct paths, thereby preventing the attacker from identifying the correct one. In addition, active RIS could be used to amplify only the signal directed to the legitimate user [28].

#### 4.2.2. Friendly Jamming

Friendly Jamming, also known as artificial noise, consists of the insertion of jamming signals into the communications channel from sources that are considered “friendly”, such as other base stations in the network, and which do not compromise the integrity of the communications. In fact, these jamming signals are designed to disrupt a potential attacker, making it difficult for them to decipher the message or attempt to interfere. Despite the jamming, the receiver manages to receive the signal undisturbed. This is achieved by modulation techniques as described in [29]. In this article, Friendly Jamming is applied to MIMO-OFDM (Multiple-Input, Multiple-Output Orthogonal Frequency-Division Multiplexing) systems or by using specific frequencies to filter out artificial noise. Friendly Jamming has some limitations: first, it could be subject to spoofing attacks, i.e., an attacker could spoof a friendly signal to make it indistinguishable from the real one for the detection system and thus gain access to the communication channel; a second weakness is the lack of sufficient resources to ensure reliable Friendly Jamming: this is more common in systems with limited processing capacity, such as small devices.

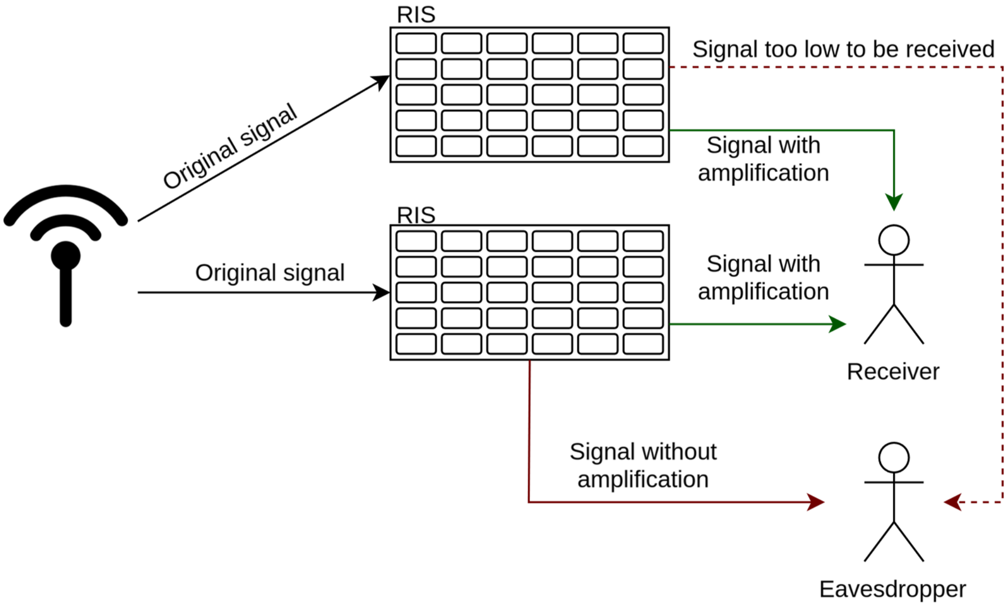
RIS
Signal too low to be received
Original signal
Signal with amplification
RIS
Original signal
Signal with amplification
Receiver
Signal without amplification
Eavesdropper

**Figure 4.** Example of an RIS-based countermeasure to the eavesdropping attack.

### 4.2.3. NOMA

NOMA (Non-Orthogonal Multiple Access) is an access technique for multiple users to communicate over the same data spectrum [30]. It achieves non-orthogonal access by spatially overlapping the signals transmitted, allowing multiple users to share time and frequency resources. This gives higher power to data with higher priority and removes it from data with lower priority, making the former more difficult to intercept and increasing their security. To receive the distinct signal, users must decode and demodulate the overlapping signals, exploiting differences in signal power levels and using advanced modulation techniques. Due to its flexibility and optimization, NOMA is particularly suitable for systems such as 6G where a large number of devices are connected and there is a need to ensure numerous simultaneous communications. Despite the high security of NOMA, some vulnerabilities could jeopardize the integrity and security of communication. One of these is the wiretapping of transmission devices through which attackers passively intercept communications. Attackers who gain control of multiple transmission devices can spy on communications passively and try to discover the modulated message by simulating the modulation technique of the intercepted channel. A further vulnerability could arise if attackers send numerous messages with high priority to allocate enough power to make it impossible for other communications to have protection. To ensure greater security and reduce the number of vulnerabilities, the literature [30] proposes several solutions. These include the implementation of Friendly Jamming and the use of RIS in the NOMA itself, both of which are particularly optimized for 6G systems.

### 4.2.4. Frequency Hopping

Frequency Hopping [31] is a technique used against PCA attacks. It is based on changing the frequency of the communication channel in an uncoordinated way. This makes it difficult for an attacker attempting to contaminate the pilot signal of the communication to identify the path of the communication and intercept it. Although an attacker may be able to detect the signal on a specific frequency, it would be impossible to completely reconstruct it due to the unknown jumps. Additionally, Zhang et al. [31] have developed an algorithm to detect a PCA, while an attacker attempts to emulate communication frequency hopping.

#### 4.2.5. Reinforcement Learning

Reinforcement Learning (RL) is a machine learning technique where an agent interacts with the environment, learning an optimal policy, by trial and error [32]. Reinforcement Learning can be a cornerstone for securing the 6G systems' physical layer. It enables the automatic optimization of security criteria by analyzing the environment through an algorithm and adjusting individual parameters. This eliminates the need to rely solely on pre-established attack patterns. Furthermore, it could be utilized to optimize previously discussed physical layer techniques, such as NOMA and Friendly Jamming. The first could be optimized through the use of RL, with an algorithm capable of selecting the appropriate transmission power for each signal, setting the optimal ratio between secrecy rate and interception probability, as demonstrated in [33]. Friendly Jamming can be optimized through beamforming, which is a technique that concentrates the signal beam in a specific direction instead of spreading it in all directions, based on RL. Through Reinforcement Learning, beamforming parameters such as orientation and intensity can be dynamically modified to adapt to the attacker's tactics and behaviors [34].

## 5. Connection Layer

The connection layer is the one responsible for managing and establishing connections between devices. It is also responsible for authenticating and discovering devices on the network and managing traffic to avoid congestion and improve QoS. Figure 5 shows the relations between the mitigations proposed and the security and trust threats.

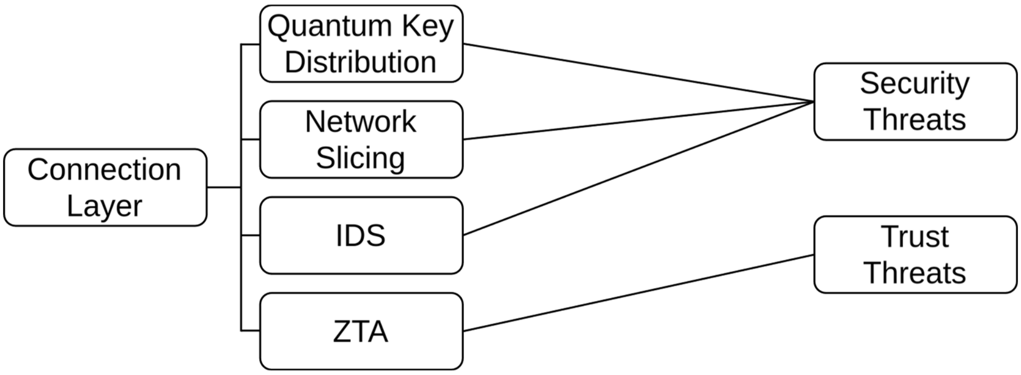

**Figure 5.** Diagram of the mitigations in the connection layer divided by security and trust threats.

### *5.1. Vulnerabilities and Threats*

The connection layer can fall victim to other types of attacks than those of the physical layer:

- DoS (Denial of Service): this attack aims to make a service, resource, or network inaccessible to legitimate users by creating an excessive volume of requests, saturating the available traffic [35].
- Distributed Denial of Service (DDoS): this is a similar type of attack to DoS but uses multiple devices to achieve higher impact by increasing the number of requests and hampering defenses based on isolating the attacker's address [36].
- MitM (Man-in-the-Middle): this is an active attack in which attackers are able to position themselves on the path between legitimate endpoints to intercept and alter communication without their knowledge [37].
- Replay Attack: in this attack, the attacker intercepts and stores communication data and then later reuses it to gain unauthorized access or to perform malicious operations [38].

### *5.2. Mitigations*

#### 5.2.1. Quantum Key Distribution

Quantum Key Distribution (QKD) uses the fundamental principles of quantum physics to generate keys that are impossible to intercept. In a QKD system, there are two key figures, the transmitter and the receiver, connected via a dual link, one classical and one quantum. In the classic channel, information is transmitted with traditional IT techniques, while in the quantum channel, data are transmitted through quantum states, e.g., the instantaneous microscopic state of individual photons that can be used to transmit information [39]. If an attacker attempts to intercept a communication on the quantum channel, the quantum states of the photons will be altered by the laws of quantum physics, consequently altering the communication. Therefore, QKD allows a more secure distribution of symmetric keys between the transmitter and receiver compared to 5G's symmetric encryption mechanism. However, this technology still has evident limitations due to the necessity of utilizing specialized equipment. Quantum Key Distribution (QKD) is based on physical principles for its security, which is derived from the distinctive characteristics of the physical layer in communications. This necessitates that users either lease dedicated fiber connections or manually manage transmitters in open space. Its implementation is not feasible via software or as a network service, and it presents challenges for seamless integration into the current network infrastructure.

#### 5.2.2. Network Slicing

Network Slicing is a technology that allows for dividing the network into multiple virtual networks each with its own resources and characteristics. The division is based on the functionality and performance of each service so that each service has specific requirements for the particular use case to which it refers. From a security point of view, Network Slicing can be used to ensure the confidentiality and control of resource consumption in a 6G system, as cross-slice communication is not allowed. Although this may seem like a limitation, it guarantees a greater level of security because any attack will be limited to a single slice and will not spread throughout the entire system. A further security mechanism consists of authenticating the managers of two network slices belonging to two different endpoints before allowing the single slice to process data, as described in [40]. Figure 6 shows a representation of how network slicing separates different kinds of traffic, adapting the transmission based on their different needs.

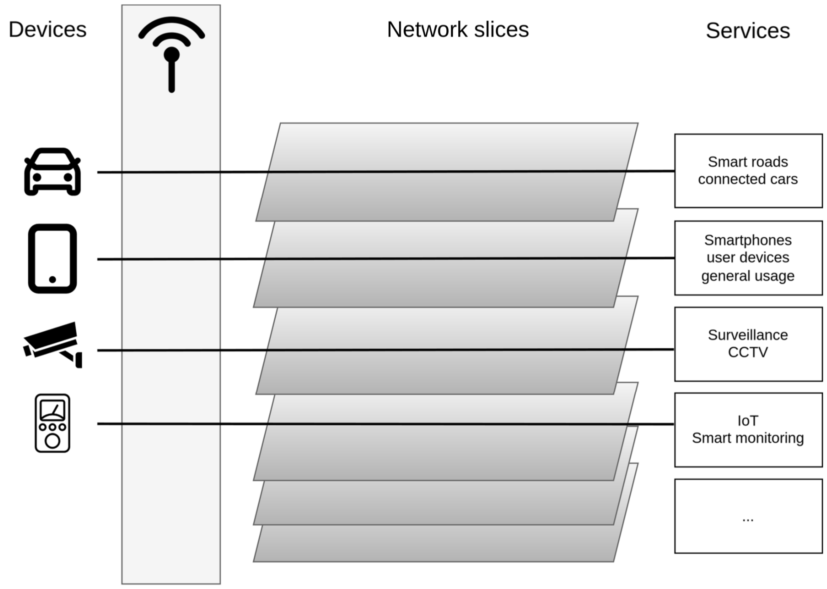

**Figure 6.** Example of how Network Slicing works.

#### 5.2.3. IDS

The IDS is a system that automates the event monitoring process, analyzing and researching security threats [41]. An IDS observes event data and detects potentially dangerous activity, and it can also prevent activities (IDPS). In 6G systems, IDS will have a fundamental role. In particular, it will focus on detection methods based on Deep Learning (DL), which is a type of machine learning that uses learning algorithms to represent processed data as a hierarchy of nested concepts [42]. Deep Learning can be applied to the IDS of 6G systems to better handle the increasing complexity and size of transmitted data. Its ability to automatically learn from complex data makes it a valuable tool. DL can be used for dimensionality reduction, which reduces the size of data while preserving its meaningful properties, and for data classification, which assigns labels to new data based on patterns learned from training data. The complexity of an Intrusion Detection System (IDS) based on Deep Learning is high due to the numerous mathematical operations involved, which require significant computing power. This can be challenging to process even with AI accelerators. Recent studies [43–45] have shown promising results, and their potential application on a large scale is becoming increasingly feasible.

### *5.3. Zero Trust Architecture (ZTA)*

Another approach to the concept of trust in 6G is that of Zero Trust Architecture. Zero Trust Architecture is a strategy based on the idea that any user, device, or system within a network can be compromised at any time and is not to be trusted. Thus placing itself on the defensive, the ZTA views the network as a continuously hostile environment and its geographic location as not relevant enough to deem it trustworthy and credible. From this assumption, a series of techniques are implemented based on tight control of network access with an analysis of the risk associated with each access request; an authentication system for each user based on location, behavior, and device to verify his or her identity with the utmost precision; and an algorithm based on machine learning that analyzes all the information transmitted in the network and modifies parameters and criteria to regulate access and authentication [46]. From the perspective of logical architecture, a ZTA consists of three basic components [47]:

- Policy Engine: evaluates the validity of a user's access request using a Trust Algorithm, which is a machine learning algorithm that greatly optimizes this process;
- Policy Administrator: cooperating with the Policy Engine, decides whether to allow or deny the access using a Trust Algorithm, automating access control with a minimal error rate;
- Policy Enforcement Point: monitors and manages links between users and resources.

As of today, the foundations of the Zero Trust Architecture have been laid, but the technologies to be implemented to achieve the requirements in a system such as 6G are still far from being fully realized. The biggest problem concerns the large-scale deployment of this architecture: it requires considerable computing power that cannot be guaranteed in every device in a heterogeneous network such as 6G. In addition, access control cannot be uniform for each network; therefore, it is necessary to implement a dynamic one: the literature proposes solutions [48] but they are still immature and not fully applicable.

## 6. Application Layer

The application or service layer acts as a middleware platform that manages the system's interactions with third-party services, such as edge computing, to ensure efficiency and responsiveness. Figure 7 shows the relations between the mitigations proposed and the security and trust threats.

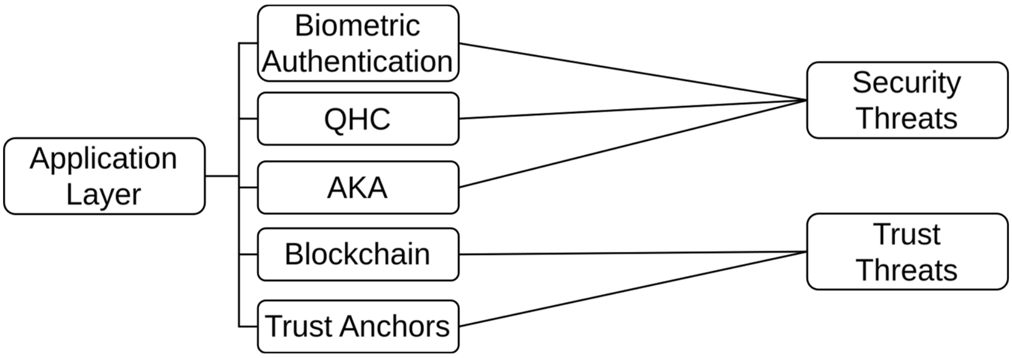

**Figure 7.** Diagram of the mitigations in the application layer divided by security and trust threats.

### *6.1. Vulnerabilities and Threats*

In addition to the sheer volume of data processed, which makes the application layer sensitive to the aforementioned DoS and DDoS attacks, the wide variety of interaction models exposes this layer to some threats that are even more difficult to counter. A peculiar threat targeting this layer, in fact, is likely to be not a purely technical one, but social engineering [49]. It consists of a series of methods used by the attacker to obtain the user's personal information through deception. There is no real method to counter social engineering, as the attacker often takes advantage of the victim's ignorance and naivety, but there are countermeasures that can reduce the ease of access to sensitive data, even in the new 6G systems, where the various connected devices will allow access to information and devices that are also particularly critical to human health.

### *6.2. Mitigations*

#### 6.2.1. Biometric Authentication

Biometric authentication [50] uses physical and behavioral properties to verify an individual's identity. There are three categories:

- Biologic, based on genetic factors of the individual;
- Morphological, based on physical traits of the individual;
- Behavioral, based on the individual's behavioral patterns.

Although biometrics have been a widely used authentication system for years, the exponential growth in computing power and advances in AI are making biometric spoofing increasingly sophisticated. As a result, to prevent potential spoofing, biometric authentication needs to ensure a higher level of authenticity. On the other hand, 6G systems are expected to significantly improve this technology, which is particularly due to the power of THz waves. These waves have high transmission capacity, enabling an unprecedented level of detail and accuracy in biometric authentication. They can facilitate the identification of individuals based on unique characteristics such as heartbeat [51] or brain waves [52].

#### 6.2.2. Quantum Homomorphic Cryptography (Qhc)

Homomorphic cryptography is an advanced cryptographic technique that allows operations to be performed on encrypted data without the need for decryption, providing extremely high security in centralized edge computing nodes. Figure 8 illustrates the phases of homomorphic cryptography in a simplified manner. A recent paper by Jonas Zeuner et al. [53] discusses a specific variant of homomorphic encryption based on the principles of quantum physics. The paper describes the use of the quantum properties of particles, such as photons, to perform operations on encrypted quantum data. Instead of conventional encryption techniques, the direction of polarization of certain photons is randomly changed to encrypt the data. The encrypted data are then transmitted to the desired service, which performs operations on it without decrypting it. Finally, the processed data are returned to the user by performing the inverse transformation. The quantum variant involves operations on particles and interpreting data through quantum states. There is little doubt about the security of QHC, and the direction for application layer cryptography is certainly geared toward it. However, there are still numerous problems to be addressed, which are particularly due to the practical implementation of quantum operations, similar to what we already noted in Section 5.2.1. This technology is still far from being fully realized.

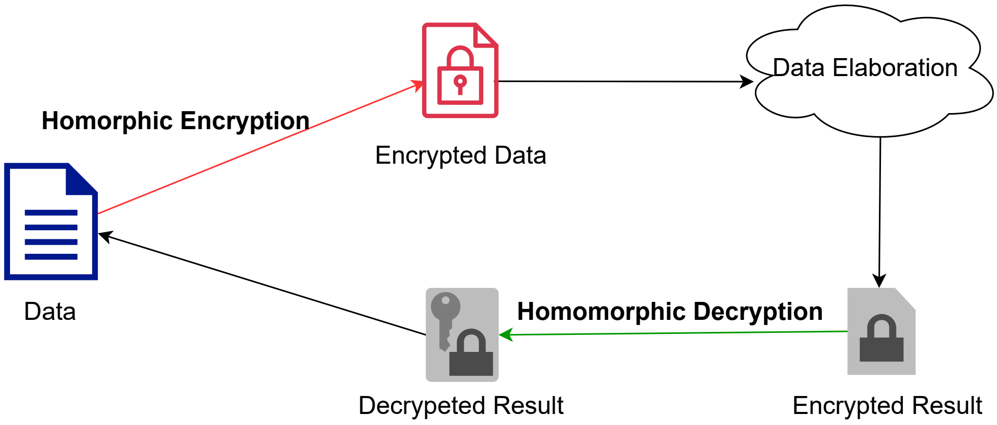

**Figure 8.** Example of homomorphic cryptography.

### 6.2.3. Authentication and Key Agreement (AKA)

Authentication and Key Agreement (AKA) is a security protocol used for mutual authentication between a device and a network provider. AKA negotiates session keys to encrypt communications between the two parties. The protocol was first used in 3G networks and has since evolved to subsequent ones, remaining the standard for mutual authentication. In 6G, the Authentication and Key Agreement protocol will need to be faster, more reliable, and provide more secure authentication. This is particularly important given the vulnerabilities that have been exposed in 5G, such as Distributed Denial of Service (DDoS) attacks [54]. Furthermore, the AKA protocol will face new challenges compared to previous network systems due to the large number of connected devices and their heterogeneous security systems. Ensuring a consistent authentication model across systems and devices with varying security capabilities presents a significant challenge. An attacker may deceive the network provider into believing that they possess a lower security capability, thereby obtaining a weaker authentication level and gaining access to sensitive data. To ensure a unique and secure authentication model, quantum algorithms will be implemented. Section 5.2.1 analyzes the quantum key distribution technique.

## *6.3. Blockchain*

A blockchain is a particular type of DLT structured as a chain of blocks containing data. The concatenation of the blocks is guaranteed by cryptography. Blockchain technology is characterized by two key principles: the Consensus Algorithm and the Smart Contract. The Consensus Algorithm is a protocol used by blockchains to establish which transactions (or blocks) to add or keep in the Distributed Ledger. Every block or transaction added to the chain must be validated by all participants (also called miners), guaranteeing integrity and creating an unbreakable bond with the other blocks or transactions in the blockchain. Thanks to this process, in the case of a large-scale blockchain, it would be almost impossible to change one part of the chain retroactively, since it would be necessary to change all the blocks subsequent to the one desired. In addition, each block keeps track of the party, making an action on the blockchain and where it came from, thus ensuring traceability on each individual transaction. There is no single Consensus Algorithm, but there are different types, each with its own advantages and disadvantages. The main ones are Proof Of Work, in which miners compete by solving cryptographic puzzles and the first to reach the answer has the right to create the new block, and Proof Of Stake, in which the one who has the most resources has the right of precedence in the creation of a new block [55].

The Smart Contract, on the other hand, is a computer program that outlines the conditions of a "contract" and in turn manages its implementation when those conditions are met. It is a useful tool because it allows specific transactions to be handled automatically when certain conditions are met and is particularly effective in areas such as programmatic banking functions and decentralized markets [56]. Blockchain technology, thanks to its many functionalities, is a crucial tool for ensuring security and reliability in modern network systems, and its application in 6G networks will be the backbone of trust in any domain: in fact, the purpose of blockchain is for every user to trust the blockchain itself so that they do not need to trust each other. As far as communications are concerned, this technology will have the dual task of ensuring the credibility of each entity on the network, assigning a trust value to each entity based on certain indicators, possibly detecting and expelling malicious ones from the network [57]; and improving the authenticity of transmitted data, using its own technologies to augment data encryption in edge computing [58].

### *6.4. Trust Anchors*

Trust Anchors are entities whose trust is predetermined and not derived from other sources. In an environment like 6G, it is crucial to have a universally recognized trusted entity among all involved parties. The architecture of a Trust Anchor can vary from a centralized to a distributed model, adapting to the needs of the network in which it is located. In order to be valid, Trust Anchors must meet certain requirements: first, they must guarantee a non-repudiation of actions within the system. That is, once a user has provided information to the Trust Anchor, he cannot go back and deny the action. Another key aspect is the ability to verify that the information saved was not compromised. Ultimately, the mechanism to verify the integrity of the information must be transparent and known to all the external users. In addition, Trust Anchors are often aided by tools called Trust and Traceability Functions (TTFs) [59], which is a particular blockchain-based service that helps establish a connection between the core of a network and its peers by storing via a distributed ledger similar to that of DLTs all communication activity in a secure manner. In addition, this service also provides a trusted logging facility that securely records the path of data exchanged during communication. However, TTFs are independent of Trust Anchors: in fact, the latter does not store user data, which is instead a task entrusted to TTFs, but focuses on verifying consensus among TTFs in distributed registries, acting as guarantors of the trustworthiness of the registries and ensuring that the information stored is authentic and verified. This division of labor provides an additional level of security and reliability in the area of data management and verification within the system. The Trust Anchors model has excellent potential for application, but the debate still remains about how to assign the label of "trustworthy" to a given Trust Anchor.

## **7. Conclusions**

Every new generation of telecommunications technology is expected to reach ever-increasing speed and capacity. The 6G technology makes no exception, but the raw performance is only the tip of the iceberg. The real game changer will be a deep integration between the network and the applications that need it. While 5G started considering the services as drivers for network configuration but still placed the burden of configuration on the network operators on request of the service providers, 6G aspires to achieve a seamless interplay between users' needs and network reaction to satisfy them. The impact of malicious behavior in such an integrated environment could be hard to contain in terms of spread and gravity. Consequently, security issues shall be taken into account at every phase of development, starting from the fundamental concepts, through the design of standards, and clearly ending in implementation. In light of this, it is of the utmost importance to conduct in-depth research into the countermeasures to be implemented in order to ensure that this new standard is as secure as possible. In our work, we undertook an analysis of the security, privacy, and trust aspects in different layers, namely the physical layer, connection layer, and application layer. This was completed in order to gain a comprehensive understanding of the security issues present in each layer and to facilitate the design of an end-to-end network security solution. Specifically, for each layer, we identified vulnerabilities, such as DoS, jamming, and pilot contamination attacks, and proposed potential mitigations, such as Friendly Jamming, Network Slicing, and QKC. It is evident that meeting real-time protection requirements and energy efficiency remain significant challenges for these technologies. Without these features, it is unlikely that many 6G security services will be able to achieve their intended objectives. In future works, it would be beneficial to examine each level of the OSI model in order to gain a more comprehensive understanding of potential security issues.

**Author Contributions:** Conceptualization, G.T., A.I. and L.R.; Methodology, G.T., A.I. and L.R.; Validation G.T., A.I. and L.R.; Writing—original draft, G.T. and A.I.; Writing—review and editing, L.R. and M.P.; Supervision, M.P. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union—NextGenerationEU and by the IGNITE5.0 project funded by the Emilia-Romagna region in the framework of the POR-FESR 2021-2027 program (the EU program for regional development).

**Data Availability Statement:** Data is contained within the article.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| AI | Artificial Intelligence |
| AKA | Authentication Key Agreement |
| BCI | Wireless Brain–Computer Interactions |
| CRAS | Connected Robotics and Autonomous Systems |
| DDoS | Distributed Denial of Service |
| DL | Deep Learning |
| DLT | Distributed Ledger Technologies |
| DoS | Denial of Service |
| IDPS | Intrusion Detection and Prevention System |
| IDS | Intrusion Detection System |
| IoT | Internet of Things |
| MIMO-OFDM | Multiple-Input, Multiple-Output Orthogonal Frequency-Division Multiplexing |
| MitM | Man-in-the-Middle |
| NOMA | Non-Orthogonal Multiple Access |
| PCA | Pilot Contamination Attacks |
| QHC | Quantum Homomorphic Cryptography |
| QKD | Quantum Key Distribution |
| QoS | Quality of Service |
| RIS | Reconfigurable Intelligent Surfaces |
| RL | Reinforcement Learning |
| TTFs | Trust and Traceability Functions |
| VLC | Visible Light Communication |
| XR | eXtended Reality |
| ZTA | Zero Trust Architecture |

## References

1. GSMA. The Mobile Economy 2024. 2024. Available online: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/02/260224-The-Mobile-Economy-2024.pdf (accessed on 17 April 2024),
2. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236.

3. Sun, Y.; Liu, J.; Wang, J.; Cao, Y.; Kato, N. When machine learning meets privacy in 6G: A survey. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 2694–2724.
4. Sheth, K.; Patel, K.; Shah, H.; Tanwar, S.; Gupta, R.; Kumar, N. A taxonomy of AI techniques for 6G communication networks. *Comput. Commun.* **2020**, *161*, 279–303.
5. Ylianttila, M.; Kantola, R.; Gurtov, A.; Mucchi, L.; Oppermann, I.; Yan, Z.; Nguyen, T.H.; Liu, F.; Hewa, T.; Liyanage, M.; et al. 6G white paper: Research challenges for trust, security and privacy. *arXiv* **2020**, arXiv:2004.11665.
6. Mitev, M.; Chorti, A.; Poor, H.V.; Fettweis, G.P. What Physical Layer Security Can Do for 6G Security. *IEEE Open J. Veh. Technol.* **2023**, *4*, 375–388. https://doi.org/10.1109/OJVT.2023.3245071.
7. Mucchi, L.; Jayousi, S.; Caputo, S.; Panayirci, E.; Shahabuddin, S.; Bechtold, J.; Morales, I.; Stoica, R.A.; Abreu, G.; Haas, H. Physical-Layer Security in 6G Networks. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1901–1914. https://doi.org/10.1109/OJCOMS.2021.3103735.
8. Xie, N.; Chen, J.; Huang, L. Physical-layer authentication using multiple channel-based features. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 2356–2366.
9. Porambage, P.; Gür, G.; Osorio, D.P.M.; Liyanage, M.; Gurtov, A.; Ylianttila, M. The roadmap to 6G security and privacy. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1094–1122.
10. Nguyen, V.L.; Lin, P.C.; Cheng, B.C.; Hwang, R.H.; Lin, Y.D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2384–2428. https://doi.org/10.1109/COMST.2021.3108618.
11. David, K.; Berndt, H. 6G Vision and Requirements: Is There Any Need for Beyond 5G? *IEEE Veh. Technol. Mag.* **2018**, *13*, 72–80. https://doi.org/10.1109/MVT.2018.2848498.
12. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Niyato, D.; Dobre, O.; Poor, H.V. 6G Internet of Things: A Comprehensive Survey. *IEEE Internet Things J.* **2022**, *9*, 359–383. https://doi.org/10.1109/JIOT.2021.3103320.
13. Jiang, W.; Han, B.; Habibi, M.A.; Schotten, H.D. The Road Towards 6G: A Comprehensive Survey. *IEEE Open J. Commun. Soc.* **2021**, *2*, 334–366. https://doi.org/10.1109/OJCOMS.2021.3057679.
14. Rappaport, T.S.; Xing, Y.; Kanhere, O.; Ju, S.; Madanayake, A.; Mandal, S.; Alkhateeb, A.; Trichopoulos, G.C. Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond. *IEEE Access* **2019**, *7*, 78729–78757. https://doi.org/10.1109/ACCESS.2019.2921522.
15. Bilotti, F.; Barbuto, M.; Hamzavi-Zarghani, Z.; Karamirad, M.; Longhi, M.; Monti, A.; Ramaccia, D.; Stefanini, L.; Toscano, A.; Vellucci, S. Reconfigurable intelligent surfaces as the key-enabling technology for smart electromagnetic environments. *Adv. Phys. X* **2024**, *9*, 2299543. https://doi.org/10.1080/23746149.2023.2299543.
16. Chi, N.; Zhou, Y.; Wei, Y.; Hu, F. Visible Light Communication in 6G: Advances, Challenges, and Prospects. *IEEE Veh. Technol. Mag.* **2020**, *15*, 93–102. https://doi.org/10.1109/MVT.2020.3017153.
17. Ziegler, V.; Schneider, P.; Viswanathan, H.; Montag, M.; Kanugovi, S.; Rezaki, A. Security and Trust in the 6G Era. *IEEE Access* **2021**, *9*, 142314–142327.
18. Liu, Y.; Yuan, X.; Xiong, Z.; Kang, J.; Wang, X.; Niyato, D. Federated learning for 6G communications: Challenges, methods, and future directions. *China Commun.* **2020**, *17*, 105–118.
19. Saad, W.; Bennis, M.; Chen, M. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Net.* **2019**, *34*, 134–142. https://doi.org/10.1109/MNET.001.1900287.
20. Minopoulos, G.; Psannis, K.E. Opportunities and Challenges of Tangible XR Applications for 5G Networks and Beyond. *IEEE Consum. Electron. Mag.* **2023**, *12*, 9–19. https://doi.org/10.1109/MCE.2022.3156305.
21. Hu, H.; Chen, X.; Jiang, T. Guest editorial: Brain-computer-interface inspired communications. *China Commun.* **2022**, *19*, iii–v. https://doi.org/10.23919/JCC.2022.9722767.
22. Baskaran, S.B.M.; Faisal, T.; Wang, C.; Lopez, D.R.; Ordonez-Lucena, J.; Arribas, I. The Role of DLT for Beyond 5G Systems and Services: A Vision. *IEEE Commun. Stand. Mag.* **2023**, *7*, 32–38. https://doi.org/10.1109/MCOMSTD.0004.2200053.
23. Cao, J.; Ma, M.; Li, H.; Ma, R.; Sun, Y.; Yu, P.; Xiong, L. A Survey on Security Aspects for 3GPP 5G Networks. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 170–195. https://doi.org/10.1109/COMST.2019.2951818.
24. López, O.L.A.; Alves, H.; Souza, R.D.; Montejo-Sánchez, S.; Fernández, E.M.G.; Latva-Aho, M. Massive Wireless Energy Transfer: Enabling Sustainable IoT Toward 6G Era. *IEEE Internet Things J.* **2021**, *8*, 8816–8835. https://doi.org/10.1109/JIOT.2021.3050612.
25. Wei, Z.; Liu, F.; Masouros, C.; Su, N.; Petropulu, A.P. Toward Multi-Functional 6G Wireless Networks: Integrating Sensing, Communication, and Security. *IEEE Commun. Mag.* **2022**, *60*, 65–71. https://doi.org/10.1109/MCOM.002.2100972.
26. Vaishnavi, K.N.; Khorvi, S.D.; Kishore, R.; Gurugopinath, S. A Survey on Jamming Techniques in Physical Layer Security and Anti-Jamming Strategies for 6G. In Proceedings of the 2021 28th International Conference on Telecommunications (ICT), London,UK, 1–3 June 2021 ; pp. 174–179. https://doi.org/10.1109/ICT52184.2021.9511465.
27. Akgun, B.; Krunz, M.; Koyluoglu, O.O. Pilot contamination attacks in massive MIMO systems. In Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 9–11 October 2017. https://doi.org/10.1109/CNS.2017.8228655.
28. Zhang, S.; Gao, H.; Su, Y.; Cheng, J.; Jo, M. Intelligent Mixed Reflecting/Relaying Surface-Aided Secure Wireless Communications. *IEEE Trans. Veh. Technol.* **2024**, *73*, 532–543. https://doi.org/10.1109/TVT.2023.3300843.

29. Cepheli, Ö.; Kurt, G.K. Efficient PHY layer security in MIMO-OFDM: Spatiotemporal selective artificial noise. In Proceedings of the 2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Madrid, Spain, 4–7 June 2013; pp. 1–6. https://doi.org/10.1109/WoWMoM.2013.6583468.
30. Furqan, H.M.; Hamamreh, J.; Arslan, H. Physical layer security for NOMA: Requirements, merits, challenges, and recommendations. *arXiv* **2019**, arXiv:1905.05064.
31. Zhang, W.; Lin, H.; Zhang, R. Detection of pilot contamination attack based on uncoordinated frequency shifts. *IEEE Trans. Commun.* **2018**, *66*, 2658–2670.
32. Kaelbling, L.P.; Littman, M.L.; Moore, A.W. Reinforcement learning: A survey. *J. Artif. Intell. Res.* **1996**, *4*, 237–285.
33. Xiao, L.; Li, Y.; Dai, C.; Dai, H.; Poor, H.V. Reinforcement learning-based NOMA power allocation in the presence of smart jamming. *IEEE Trans. Veh. Technol.* **2017**, *67*, 3377–3389.
34. Xiao, L.; Sheng, G.; Liu, S.; Dai, H.; Peng, M.; Song, J. Deep reinforcement learning-enabled secure visible light communication against eavesdropping. *IEEE Trans. Commun.* **2019**, *67*, 6994–7005.
35. Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. Denial of service attacks in wireless networks: The case of jammers. *IEEE Commun. Surv. Tutor.* **2010**, *13*, 245–257.
36. Mirkovic, J.; Reiher, P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM Sigcomm Comput. Commun. Rev.* **2004**, *34*, 39–53.
37. Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2027–2051.
38. Syverson, P. A taxonomy of replay attacks [cryptographic protocols]. In Proceedings of the Computer Security Foundations Workshop VII, Franconia, NH, USA, 14–16 June 1994; pp. 187–191.
39. Bae, J.; Kwek, L.C. Quantum state discrimination and its applications. *J. Phys. Math. Theor.* **2015**, *48*, 083001.
40. 5G Americas. *The Evolution of Security in 5G, a Slice of Mobile Threats*; 5G Americas: Bellevue, MA, USA, 2019.
41. Liao, H.J.; Lin, C.H.R.; Lin, Y.C.; Tung, K.Y. Intrusion detection system: A comprehensive review. *J. Netw. Comput. Appl.* **2013**, *36*, 16–24.
42. LeCun, Y.; Bengio, Y.; Hinton, G. Deep learning. *Nature* **2015**, *521*, 436–444.
43. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685.
44. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine learning and deep learning methods for cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381.
45. Aldweesh, A.; Derhab, A.; Emam, A.Z. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowl. Based Syst.* **2020**, *189*, 105124.
46. He, Y.; Huang, D.; Chen, L.; Ni, Y.; Ma, X. A survey on zero trust architecture: Challenges and future trends. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6476274.
47. Syed, N.F.; Shah, S.W.; Shaghaghi, A.; Anwar, A.; Baig, Z.; Doss, R. Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access* **2022**, *10*, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679.
48. Vanickis, R.; Jacob, P.; Dehghanzadeh, S.; Lee, B. Access Control Policy Enforcement for Zero-Trust-Networking. In Proceedings of the 2018 29th Irish Signals and Systems Conference (ISSC), Belfast, UK, 21–22 June 2018; pp. 1–6. https://doi.org/10.1109/ISSC.2018.8585365.
49. Salahdine, F.; Kaabouch, N. Social engineering attacks: A survey. *Future Inter.* **2019**, *11*, 89.
50. Weaver, A. Biometric authentication. *Computer* **2006**, *39*, 96–97. https://doi.org/10.1109/MC.2006.47.
51. Arnau-González, P.; Katsigiannis, S.; Arevalillo-Herráez, M.; Ramzan, N. BED: A new data set for EEG-based biometrics. *IEEE Internet Things J.* **2021**, *8*, 12219–12230.
52. Arteaga-Falconi, J.S.; Al Osman, H.; El Saddik, A. ECG authentication for mobile devices. *IEEE Trans. Instrum. Meas.* **2015**, *65*, 591–600.
53. Zeuner, J.; Pitsios, I.; Tan, S.H.; Sharma, A.N.; Fitzsimons, J.F.; Osellame, R.; Walther, P. Experimental quantum homomorphic encryption. *Npj Quantum Inf.* **2021**, *7*, 25.
54. Fei, T.; Wang, W. The vulnerability and enhancement of AKA protocol for mobile authentication in LTE/5G networks. *Comput. Net.* **2023**, *228*, 109685.
55. Du, M.; Ma, X.; Zhang, Z.; Wang, X.; Chen, Q. A review on consensus algorithm of blockchain. In Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017; pp. 2567–2572. https://doi.org/10.1109/SMC.2017.8123011.
56. Schär, F. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. In Proceedings of the Federal Reserve Bank of St. Louis Review, Second Quarter 2021, 31 March 2021; pp. 153–174. Available online: https://ssrn.com/abstract=3571335 (accessed on 30 May 2024).
57. Cinque, M.; Esposito, C.; Russo, S. Trust Management in Fog/Edge Computing by Means of Blockchain Technologies. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canda, 30 July–3 August 2018; pp. 1433–1439. https://doi.org/10.1109/Cybermatics_2018.2018.00244.

58. Zhaofeng, M.; Xiaochang, W.; Jain, D.K.; Khan, H.; Hongmin, G.; Zhen, W. A Blockchain-Based Trusted Data Management Scheme in Edge Computing. *IEEE Trans. Ind. Inform.* **2020**, *16*, 2013–2021. https://doi.org/10.1109/TII.2019.2933482.
59. Krummacker, D.; Veith, B.; Lindenschmitt, D.; Schotten, H.D. DLT architectures for trust anchors in 6G. *Ann. Telecommun.* **2023**, *78*, 551–560. https://doi.org/10.1007/s12243-022-00941-8.

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.